RED SKY ALLIANCE

TLP GREEN

TACTICAL CYBER INTELLIGENCE REPORT

Serial: TR-21-142-002
Report Date: 052321
Country: US

Iranian Ransomware Groups target Israel

Iranian hackers have reportedly hit multiple Israeli companies with ransomware, in a new campaign of attacks. A group describing itself as 'N3tw0rm' (Networm) recently added the logo of H&M Israel to their naming and shaming website, just three days after another local firm, Veritas Logistics, was hit.

It is suspected that Iran's Islamic Revolutionary Guard Corps was behind a ransomware campaign that used a contracting company called "Emen Net Pasargard," or ENP, to target over a dozen organizations, according to three leaked intelligence documents assessed by the security firm Flashpoint.

Flashpoint's report notes, however, that inclusion of financial payment steps may be a ploy to mimic the tactics, techniques and procedures of other financially motivated cybercriminal ransomware groups in an attempt to disguise the Iranian military's involvement in cyberespionage.

"Other Iranian APT groups use similar techniques to blend in with the cybercriminal threat landscape," the report states. "For example, APT33 is known to use publicly available remote access Trojans, like Nanocore, to blend in with normal cybercriminal activity and avoid the attribution which typically comes from the implementation of custom malware."

Networm is threatening to publish 110GB of data stolen from the fashion retailer and 9GB from transport firm Veritas, including information on customers, invoices, employees and possibly payment data, according to *Haaretz, a leading Israeli newspaper.* The group reportedly demanded 3 Bitcoin ($168,000) from Veritas Logistics to delete the data.

An Israel based cybersecurity firm that *Haaretz* intervired claimed it was providing incident response for three Israeli companies that had recently been hit by ransomware. There are suspicions an unnamed non-profit may also have been targeted in the ongoing campaign.

The Networm group has been linked to 'Pay2Key' an Iranian cyber-attack group that hit scores of Israeli firms at the end of last year in what some commentators described as an ideological rather than financially motivated operation. Investigators note that analyzing Pay2Key ransomware operation, they were unable to correlate it to any other existing ransomware strain, and it appears to be developed from scratch.

Several versions of this crypto-locking malware have already been spotted in the wild, which means that it is likely still under development.

If that is true, the attackers have no intention of releasing the stolen information but instead want to undermine the status of Israel as a pre-eminent cyber power, the report claimed.

In fact, it is not uncommon for ransomware threat actors to hold onto some or all of the data they've stolen. A Sophos report recently stated that although a third (32%) of victim organizations now elect to pay, only 8% got all their data back last year and 29% did not manage to grab more than half of what they lost.

Red Sky Alliance has been has analyzing and documenting cyber threats and groups for over 9 years and maintains a resource library of malware and cyber actor reports available at https://redskyalliance.org at no charge. Many past tactics are reused in current malicious campaigns.

To protect your own supply chain, consider subscribing to RedXray, Red Sky Alliance's cyber threat notification service. Details can be found at: https://www.wapacklabs.com/redxray.

Red Sky Alliance is a Cyber Threat Analysis and Intelligence Service organization. For questions, comments or assistance, please contact the office directly at 1-844-492-7225, or feedback@wapacklabs.com

Weekly Cyber Intelligence Briefings:

- Reporting: https://www.redskyalliance.org/
- Website: https://www.wapacklabs.com/
- LinkedIn: https://www.linkedin.com/company/64265941

Weekly Cyber Intelligence Briefings:

REDSHORTS - Weekly Cyber Intelligence Briefings
https://attendee.gotowebinar.com/register/3702558539639477516

https://www.infosecurity-magazine.com/news/suspected-iranian-ransomware-group/

https://www.bankinfosecurity.com/irans-military-reportedly-backs-ransomware-campaign-a-16517?rf=2021-05-05_ENEWS_SUB_BIS__Slot9_ART16517&mkt_tok=MDUxLVpYSS0yMzcAAAF82_hMoER2-

5OzOUyfmN1Vm8VomVFH2UA66s_7q4XD_Br40khvKe3R5IzAZebmFMQ18sMysgX7WU_pPGnysRH3432d5_pabCQ9JZkvcY1b2tLnq9k